CLAIMS

What is claimed is:

1   1.   A method, comprising:

2   authenticating, during a pre-boot phase of a client, a boot server on which an

3   operating system (OS) boot image is stored;

4   downloading an OS boot image from the boot server if it is authenticated; and

5   loading the OS boot image on the client;

1   2.   The method of claim 1, wherein the boot server is authenticated by comparing

2   a shared secret stored by the client with a corresponding shared secret stored by the

3   boot server.

1   3.   The method of claim 2, further comprising provisioning the shared secret to at

2   least one of the client and the boot server during a one-time provisioning event such

3   that both the client and the boot server have access to the shared secret.

1   4.   The method of claim 3, wherein the shared secret is provisioned using an

2   Extensible Authentication Protocol (EAP message) exchange between an

3   authenticator EAP server and the client.

1   5.   The method of claim 3, wherein the shared secret is provisioned from the

2   client to the server and is formulated via a key that is generated by a trusted platform

3   module stored by the client.

1   6.   The method of claim 3, wherein the shared secret is provisioned using a take

2   ownership protocol under which one of a user or administrator takes ownership of a

3   computer system by providing authentication credentials for that system..

1   7.   The method of claim 6, wherein the take ownership protocol comprises

2   provisioning authentication credentials via one of the following: provisioning

3   authentication credentials on the client via an out-of-band channel, enabling a user

4   to enter authentication credentials via a local console, and imprinting the client with

5   authentication credentials via remote entry of the authentication credentials by a

6   system administrator.

1   8.   The method of claim 1, wherein the boot server is authenticated using an

2   authenticated dynamic host configuration protocol (DHCP) message exchange

3   process.

1   9.   The method of claim 1, further comprising authenticating the client prior to

2   allowing a client to download an OS boot image.

1   10.   The method of claim 9, wherein the client is authenticated using an

2   authenticated dynamic host configuration protocol (DHCP) message exchange

3   process.

1   11.   The method of claim 1, wherein the boot server is authenticated by

2   performing the operations of:

3   encrypting the shared secret stored at the client;

4   passing the encrypted shared secret to one of the boot server and an

5   authentication proxy for the boot server;

6   decrypting the encrypted shared secret at said one of the boot server and the

7   proxy for the boot server; and

8   comparing a shared secret stored at said one of the boot server and the

9   authentication proxy for the boot server with the encrypted shared secret that is

10   decrypted.

1   12.   The method of claim 1, further comprising:

2   generating a session key; and

3   employing the session key for encryption and decryption of data transferred

4   between the boot server and the client.

1   13.   The method of claim 12, further comprising:

2   updating the session key at some point during download of the OS boot

3   image; and

4   employing the updated session key for encryption and decryption of data

5   transferred between the boot server and the client while downloading a subsequent

6   portion of the OS boot image.

1   14.   The method of claim 1, wherein the shared secret is derived from the

2   combination of a user login and a password corresponding to the user login.

1   15.   A computer system, comprising:

2   a processor;

3   memory, coupled to the processor;

4   a network interface, coupled to the processor;

5   a firmware storage device, coupled to the processor; having firmware

6   instructions stored therein that when executed on the processor cause operations to

7   be performed, including:

8   interacting with a boot server via messages sent to and received from

9   the boot server through the network interface during a pre-boot initialization

10   phase of the computer system to authenticate the boot server;

11   downloading an OS boot image from the boot server if it is

12   authenticated; and

13   loading the OS boot image into the memory.

1   16.   The system of claim 15, wherein the boot server is authenticated by

2   comparing a shared secret stored by the computer system with a corresponding

3   shared secret stored by the boot server.

1   17.   The system of claim 15, wherein the boot server is authenticated using an

2   authenticated dynamic host configuration protocol (DHCP) message exchange

3   process.

1   18.   The system of claim 17, wherein execution of the firmware instructions further

2   performs authentication of the computer system via the authenticated DHCP

3   message exchange process.

1   19.   The system of claim 15, wherein the OS boot image is served from the boot

2   server in an encrypted form, and execution of the firmware instructions further

3   performs the operation of decrypting the OS boot image.

1　20.　The system of claim 19, wherein execution of the firmware instructions further

2　performs the operation of interacting, via a message exchange, with the boot server

3　to agree on a session key that is used to encrypt and decrypt the OS boot image.

1　21.　The system of claim 15, further comprising a trusted platform module,

2　operatively coupled to the processor and storing an ownership token that is used to

3　formulate the shared secret.

1　22.　The system of claim 21, wherein the ownership token comprises a key that is

2　instantiated via the trusted platform module.

1　23.　A machine-readable media providing instructions to perform operations on a

2　computer system, including:

3　　　　　interacting with one of a boot server or authentication server via

4　　　　messages generated by the computer system and sent to the boot server or

5　　　　authentication server and messages received from the boot server or

6　　　　authentication server and processed by the computer system during a pre-

7　　　　boot initialization phase of the computer system to authenticate the boot

8　　　　server;

9　　　　　sending a request to the boot server to download an OS boot image

10　　　　from the boot server if it is authenticated;

11　　　　　downloading the OS boot image from the boot server; and

12　　　　　loading the OS boot image into memory of the computer system.

1　24.　The machine-readable media of claim 23, wherein the media comprises a

2　firmware storage device and the instructions comprise firmware instructions.

1   25.   The machine-readable media of claim 23, wherein execution of the

2   instructions performs the further operation of broadcasting a boot server discovery

3   message to locate the boot server.

1   26.   The machine-readable media of claim 23, wherein the boot server is

2   authenticated by comparing a shared secret stored by the computer system with a

3   corresponding shared secret stored by the boot server.

1   27.   The machine-readable media of claim 26, wherein execution of the

2   instructions performs the further operations of:

3   encrypting the shared secret stored at the computer system; and

4   sending the shared secret in encrypted form to one of the boot server or an

5   authentication proxy for the boot server.

1   28.   The machine-readable media of claim 23, wherein the boot server is

2   authenticated using an authenticated dynamic host configuration protocol (DHCP)

3   message exchange process.

1   29.   The machine-readable media of claim 28, wherein execution of the

2   instructions further performs authentication of the computer system via the

3   authenticated DHCP message exchange process.

1   30.   The machine-readable media of claim 23, wherein execution of the

2   instructions further performs the operations of:

3   generating a user interface on the computer system via which a user can

4   enter authentication credentials;

5   generating a shared secret based on the authentication credentials; and

6   sending the shared secret to the boot server or authentication server.